



IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
MEWE.COM ACCOUNTS, "GREG W"
(GREGW62@HOTMAIL.COM) AND
"BUZZA W" (GREGW62@YMAIL.COM),
THAT IS STORED AT PREMISES
CONTROLLED BY MEWE.COM

2:20-mj-00047

Case No. _____

Filed Under Seal

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Michael D. Fleener, being duly sworn, do hereby depose and
state as follows:

I. INTRODUCTION

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been so employed since April 2001 (formerly U.S. Customs Service). I am currently assigned to the Office of the Resident Agent in Charge, in Charleston, West Virginia. Prior to becoming a Special Agent, I was employed as a police officer in Lexington, Kentucky, from July 1995 to March 2001. I also served in the United States Marine Corps as a military police officer from April 1990 to July 1995. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. For the past 16

years, I have investigated violations of federal law including the online exploitation of minors, particularly in relation to violations of Title 18, United States Code, Sections 2251, 2252A and 2423(b) and (c). I have participated in the execution of search warrants involving child exploitation and child pornography offenses, and the search and seizure of computers and other digital devices related to those offenses. I am a member of the West Virginia Internet Crimes Against Children ("WV ICAC") Task Force and work with other federal, state, and local law enforcement personnel in the investigation of crimes involving the sexual exploitation of children.

II. PURPOSE OF THE AFFIDAVIT

2. The statements contained in this affidavit are based on my knowledge or information provided by MeWe.com and the National Center for Missing and Exploited Children (NCMEC). This affidavit is being submitted for the limited purpose of securing a search warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause that violations of Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography; 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce, have occurred in Boone County, West Virginia, within the

Southern District of West Virginia, and that evidence of those violations is presently stored at the premises owned, controlled or operated by MeWe.com, an electronic service provided headquartered at 11874 Juniette Street, Culver City, CA 90230.

III. STATUTORY AUTHORITY

3. The investigation concerns potential violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B), relating to matters involving the sexual exploitation of minors.

- a. 18 U.S.C. 2252A (a)(1) prohibits any person from knowingly mailing, transporting, or shipping child pornography in interest or foreign commerce by any means, including by computer.
- b. 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- c. 18 U.S.C § 2252A(a)(5)(B) prohibits any person from knowingly possessing any book, magazines, periodicals films, video tapes computer disk or other matter that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means including computer, or that was produced using materials mailed, or shipped or transported in interstate or foreign commerce by any means including computer.

4. The following definitions apply to this Affidavit and its Attachments.

- a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
- c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- d. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where
 - i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

- ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
 - iii. such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage,

and co-locations of computers and other communications equipment.

- h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an ISP assigns a user's computer a particular IP address each time the computer accesses the Internet.
- i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of www.usdoj.gov refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.
- j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- k. A "Preservation Letter" is a letter governmental entities may issue to Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers preserve records in their possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

5. The legal authority for this search warrant application is derived from 18 U.S.C. §§ 2701-2711. 18 U.S.C. § 2703(c) (A) allows for nationwide service of process of search warrants for

the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

6. This Court has jurisdiction to issue the requested warrant as it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States (including a magistrate judge or such a court) . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). The investigation reveals that there is probable cause to believe that the target, Greg Alan WEYMES, engaged in illegal conduct, as referenced in this Affidavit, from and within the Southern District of West Virginia. See 18 U.S.C. § 3237; see also 18 U.S.C. §§ 3231 and 3232.

IV. BACKGROUND REGARDING COMPUTERS, THE INTERNET AND EMAIL

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

- a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.
- b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.
- c. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.¹ Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials among pornographers.

- d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.
- e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc. and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is

¹ The File Transfer Protocol ("FTP") is a protocol that defines how files are transferred from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

used, however, evidence of child pornography can often be found on the user's computer.

- g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

V. BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE

8. Based on my training and experience, and publicly-available information, I know that the National Center for Missing and Exploited Children ("NCMEC") is a nonprofit, nongovernmental organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC

is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

9. In addition to reports from the general public, Title 18, United States Code, Section 2258A requires all providers of an electronic communication service or remote computing service to the public through a facility or means of interstate or foreign commerce, to report "apparent child pornography" to NCMEC via the CyberTipline. Leads are reviewed by specially-trained analysts, who examine and evaluate the reported content, add related information that may be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

10. The CyberTipline receives reports, known as CyberTip Reports, on the following types of criminal conduct: possession, manufacture and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

11. The CyberTip Reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any

individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an electronic communication service or remote commuting service uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. See 18 U.S.C. § 2258A(b). Also, as will be illustrated below, CyberTip Reports can be supplemented and made in connection with other CyberTip Reports.

VI. BACKGROUND ON MeWe.com

12. MeWe.com is a social networking website and cellular phone application that was launched in 2016 and is owned and operated by technology company Sgrouples, Inc. based in Culver City, California. MeWe.com developed in order to allow individuals with similar interests to connect online and in person. MeWe.com allows registered users to utilize the social media platform on any internet capable and/or mobile devices. MeWe.com touts itself as a social media platform that is focused on the privacy of its users and does not sell the information of

its users to third parties. In order to use the website/application, a user must first register on MeWe.com. To do this, the user designates a username that will serve as their username to communicate with other users. The user must also designate either a cellular phone number or an email address in order to verify registration as a MeWe.com user. Once the user provides either a phone number or an email address, MeWe.com sends a code to either the cellular phone in the form of a text message or by email, depending on which confirmation method the user chose to provide to MeWe.com during the registration process. During the registration process, the user must acknowledge having read the terms of service that outline (among other prohibitions) that posting any pornographic content on MeWe.com is prohibited, and that MeWe.com monitors the transmissions of its users to ensure compliance with the terms of use. After completing the registration process, users can communicate online via text and/or chat group and send/receive pictures and videos.

13. Most of the social networking and remote storage software applications keep logs of each upload, access, and/or download event. Often a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained, uploaded, or downloaded. MeWe.com, like most other social media applications, has developed a monitoring system to detect if their service may have been used to transmit or store child pornography.

Once MeWe.com detects and logs the transmission of child pornography by one of its users, MeWe.com makes a report to NCMEC of the date, time, and IP address(es) of the transmission. MeWe.com also provides the content of the suspected illegal transmission.

VII. FACTS ESTABLISHING PROBABLE CAUSE

14. On January 14, 2020, HSI in Charleston, West Virginia received information from NCMEC, documented in CyberTipline report 58504599, regarding MeWe.com account "Greg W", also identified by email address gregw62@hotmail.com.

15. The report was filed with NCMEC on October 31, 2019 by representatives of MeWe.com and documented that from October 1, 2019, 13:38:05 UTC (Coordinated Universal Time) through October 2, 2019, 21:18:19 UTC, MeWe user "Greg W" uploaded 22 (twenty-two) image files believed to contain child pornography. The image files were uploaded from Internet Protocol (IP) addresses 184.14.101.186, 209.33.121.182, 74.195.13.104, 99.203.17.209 and 108.113.229.6. The report further advised that all images were viewed by MeWe.com personnel.

16. Three of the images files are described below based on your affiant's observations of the content:

a. Image file - e1bb744c29208147af3090da52d18370.jpg depicts a female between the age of 15 and 25 years of age

performing oral sex on a nude female toddler between 2 and 3 years of age.

b. Image file- img(2).png depicts an adult female performing oral sex on a nude prepubescent male who is erect. The male appears to be between 4 and 6 years of age

c. Image file - 922a9f5e3315e92867a87dc2fdd14650.jpg depicts a prepubescent naked female, laying on her back and wearing thigh-high leg stockings that cover from her knees down, with her legs in the air. The female has a sexual toy in her right hand, inserting it into her vagina, and an adult male's penis can be seen in the foreground of the image.

17. Your affiant observed while reviewing the CT report that it was linked to a second CyberTipline report (CT 59070900) by another email address also using "gregw62" as well as IP address 74.195.13.104 and 209.33.121.182.

18. Your affiant requested CT report 59070900 from NCMEC and received that report on February 25, 2020. Upon review, CT report 59070900 was filed with NCMEC on November 6, 2019 by representatives of MeWe.com and documented that from October 12, 2019, 19:00:11 UTC (Coordinated Universal Time) through November 6, 2019, 15:57:58 UTC, MeWe.com user "buzza w" uploaded 26 (twenty-six) image files believed to contain child pornography. The image files were uploaded from many different IP addresses, but of note, 74.195.13.104 and 209.33.121.182, as mentioned in paragraph 15,

were also used to log into "buzza w" account. The report further advised that all images were viewed by MeWe.com personnel.

19. Two of the images files are described below based on your affiant's observations of the content:

a. Image file - image(2)(1)(1).jpg depicts two prepubescent female minors with a prepubescent male minor. One of the females appears nude (only the face of the second female is visible) and the female is digitally manipulating the prepubescent male's penis, which appears erect.

b. Image file - img(3).png depicts a clothed adult female performing oral sex on a prepubescent male, who is sitting upright and clothed, but his pants and underwear are pulled down.

20. Further review of report 59070900 reveals that "buzza w" registered an email account of gregw62@ymail.com.

21. On January 16, 2020, your affiant issued an administrative subpoena to Frontier Communications for subscriber information for IP address 184.14.101.186, referenced in paragraph 15, for the date and time of October 2, 2019 between 21:15:00 and 21:30:00 UTC. On January 16, 2020, Frontier Representatives responded with the following subscriber information:

IP: 184.14.101.186

Session Start: 2019-09-30 13:55:58 UTC

Session End: 2019-10-06 01:39:42 UTC

Email Address: gregw62@frontier.com

Name: Greg Weynes [sic]

Address: ~~XXXXXXXXXXXX~~, Ridgeview, WV 25169

Customer Number: ~~XXXXXXXXXX~~

Connect Date: 03-03-2016


22. West Virginia Department of Motor Vehicles show a Greg Alan WEYMES, license number ~~XXXXXXXX~~, with an address of ~~XXXXXXXXXX~~, Ridgeview, Boone County, WV 25169.

23. On February 27, 2020, your affiant submitted a request for preservation of evidence/records to MeWe.com relating to accounts for "Greg W"/gregw62@hotmail.com and "buzza w"/gregw62@ymail.com.

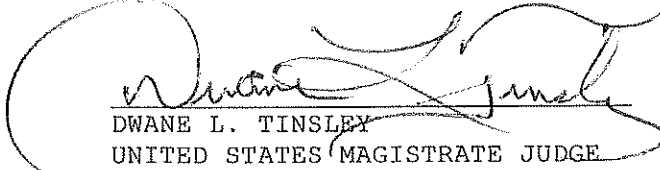
VIII. CONCLUSION

24. Based on the aforementioned factual information, and my training and experience, your affiant respectfully submits that there is probable cause to believe that the user of the MeWe.com account(s) "Greg W"/gregw62@hotmail.com and "buzza w"/gregw62@ymail.com, has committed a violation of Title 18, United States Code, Sections 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B) and that evidence of those offenses, as more fully described in Attachment B, is presently contained in the MeWe.com accounts located on the computer system or server in the control of MeWe.com. Your affiant requests MeWe.com be ordered to disclose

the above information to the government within 14 days of the issuance of this warrant.


SPECIAL AGENT MICHAEL D. FLEENER
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Subscribed and affirmed via telephonic means
on this 6th day of April, 2020:


DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE